AMENDMENTS TO THE CLAIMS

1.   (original) A method for verifying the legitimacy of an untrusted mechanism, comprising:

submitting a first set of information and a second set of information to an untrusted mechanism in a sequence that is unpredictable to the untrusted mechanism;

receiving a response from the untrusted mechanism for each submission of either said first set of information or said second set of information;

determining whether each response received from the untrusted mechanism is a correct response; and

in response to a determination that any of the responses from the untrusted mechanism is an incorrect response, determining the untrusted mechanism to not be legitimate.

2.   (original) The method of claim 1, wherein said sequence is generated randomly.

3.   (original) The method of claim 2, wherein said sequence is generated using a random number generator.

4.   (original) The method of claim 1, wherein said sequence includes at least one submission of said first set of information and at least one submission of said second set of information.

5. (original) The method of claim 1, wherein said first set of information is designed to solicit a first proper response from the untrusted mechanism, and said second set of information is designed to solicit a second proper response from the untrusted mechanism, and wherein determining whether each response received from the untrusted mechanism is a correct response comprises:

where the set of information submitted to the untrusted mechanism was said first set of information, determining whether the response from the untrusted mechanism is said first proper response; and

where the set of information submitted to the untrusted mechanism was said second set of information, determining whether the response from the untrusted mechanism is said second proper response.

6. (original) The method of claim 5, wherein said first proper response is an affirmative response, and wherein said second proper response is a negative response.

7. (original) A method for verifying the legitimacy of an untrusted signature verification mechanism, comprising:

submitting a first signature and a second signature to an untrusted signature verification mechanism in a sequence that is unpredictable to the untrusted mechanism, said first signature being known to be verifiable, and said second signature being known to be unverifiable;

receiving a response from the untrusted mechanism for each submission of either said first signature or said second signature;

determining whether each response received from the untrusted mechanism is a

correct response; and

in response to a determination that any of the responses from the untrusted

mechanism is an incorrect response, determining the untrusted mechanism

to not be legitimate.

8. (original) The method of claim 7, wherein said sequence is generated randomly.

9. (original) The method of claim 8, wherein said sequence is generated using a

random number generator.

10. (original) The method of claim 7, wherein said sequence includes at least one

submission of said first signature and at least one submission of said second

signature.

11. (original) The method of claim 7, wherein determining whether each response

received from the untrusted mechanism is a correct response comprises:

where the signature submitted to the untrusted mechanism was said first signature,

determining whether the response from the untrusted mechanism is that said

first signature is verified; and

where the signature submitted to the untrusted mechanism was said second

signature, determining whether the response from the untrusted

mechanism is that said second signature is not verified.

12.　(original) An apparatus for verifying the legitimacy of an untrusted mechanism, comprising:

　　a mechanism for submitting a first set of information and a second set of information to an untrusted mechanism in a sequence that is unpredictable to the untrusted mechanism;

　　a mechanism for receiving a response from the untrusted mechanism for each submission of either said first set of information or said second set of information;

　　a mechanism for determining whether each response received from the untrusted mechanism is a correct response; and

　　a mechanism for determining, in response to a determination that any of the responses from the untrusted mechanism is an incorrect response, the untrusted mechanism to not be legitimate.

13.　(original) The apparatus of claim 12, wherein said sequence is generated randomly.

14.　(original) The apparatus of claim 13, wherein the mechanism for submitting comprises a random number generator.

15.　(original) The apparatus of claim 12, wherein said sequence includes at least one submission of said first set of information and at least one submission of said second set of information.

16.　(original) The apparatus of claim 12, wherein said first set of information is designed to solicit a first proper response from the untrusted mechanism, and said second set of information is designed to solicit a second proper response from the untrusted mechanism, and wherein the mechanism for determining whether each response received from the untrusted mechanism is a correct response comprises:

　　a mechanism for determining, where the set of information submitted to the untrusted mechanism was said first set of information, whether the response from the untrusted mechanism is said first proper response; and

　　a mechanism for determining, where the set of information submitted to the untrusted mechanism was said second set of information, whether the response from the untrusted mechanism is said second proper response.

17.　(original) The apparatus of claim 16, wherein said first proper response is an affirmative response, and wherein said second proper response is a negative response.

18.　(original) An apparatus for verifying the legitimacy of an untrusted signature verification mechanism, comprising:

　　a mechanism for submitting a first signature and a second signature to an untrusted signature verification mechanism in a sequence that is unpredictable to the untrusted mechanism, said first signature being known to be verifiable, and said second signature being known to be unverifiable;

a mechanism for receiving a response from the untrusted mechanism for each

submission of either said first signature or said second signature;

a mechanism for determining whether each response received from the untrusted

mechanism is a correct response; and

a mechanism for determining, in response to a determination that any of the

responses from the untrusted mechanism is an incorrect response, the

untrusted mechanism to not be legitimate.

19. (original) The apparatus of claim 18, wherein said sequence is generated

randomly.

20. (original) The apparatus of claim 19, wherein the mechanism for submitting

comprises a random number generator.

21. (original) The apparatus of claim 18, wherein said sequence includes at least one

submission of said first signature and at least one submission of said second

signature.

22. (original) The apparatus of claim 18, wherein the mechanism for determining

whether each response received from the untrusted mechanism is a correct

response comprises:

a mechanism for determining, where the signature submitted to the untrusted

mechanism was said first signature, whether the response from the

untrusted mechanism is that said first signature is verified; and

a mechanism for determining, where the signature submitted to the untrusted

mechanism was said second signature, whether the response from the

untrusted mechanism is that said second signature is not verified.

23. (original) A computer readable medium having stored thereon instructions which,

when executed by one or more processors, cause the one or more processors to

verify the legitimacy of an untrusted mechanism, said computer readable medium

comprising:

instructions for causing one or more processors to submit a first set of information

and a second set of information to an untrusted mechanism in a sequence

that is unpredictable to the untrusted mechanism;

instructions for causing one or more processors to receive a response from the

untrusted mechanism for each submission of either said first set of

information or said second set of information;

instructions for causing one or more processors to determine whether each

response received from the untrusted mechanism is a correct response; and

instructions for causing one or more processors to determine, in response to a

determination that any of the responses from the untrusted mechanism is

an incorrect response, the untrusted mechanism to not be legitimate.

24. (original) The computer readable medium of claim 23, wherein said sequence is

generated randomly.

25. (original) The computer readable medium of claim 24, wherein said sequence is generated using a random number generator.

26. (original) The computer readable medium of claim 23, wherein said sequence includes at least one submission of said first set of information and at least one submission of said second set of information.

27. (original) The computer readable medium of claim 23, wherein said first set of information is designed to solicit a first proper response from the untrusted mechanism, and said second set of information is designed to solicit a second proper response from the untrusted mechanism, and wherein the instructions for causing one or more processors to determine whether each response received from the untrusted mechanism is a correct response comprises:

instructions for causing one or more processors to determine, where the set of information submitted to the untrusted mechanism was said first set of information, whether the response from the untrusted mechanism is said first proper response; and

instructions for causing one or more processors to determine, where the set of information submitted to the untrusted mechanism was said second set of information, whether the response from the untrusted mechanism is said second proper response.

28.   (original) The computer readable medium of claim 27, wherein said first proper

response is an affirmative response, and wherein said second proper response is a

negative response.

29.   (original) A computer readable medium having stored thereon instructions which,

when executed by one or more processors, cause the one or more processors to

verify the legitimacy of an untrusted signature verification mechanism, said

computer readable medium comprising:

instructions for causing one or more processors to submit a first signature and a

second signature to an untrusted signature verification mechanism in a

sequence that is unpredictable to the untrusted mechanism, said first

signature being known to be verifiable, and said second signature being

known to be unverifiable;

instructions for causing one or more processors to receive a response from the

untrusted mechanism for each submission of either said first signature or

said second signature;

instructions for causing one or more processors to determine whether each

response received from the untrusted mechanism is a correct response; and

instructions for causing one or more processors to determine, in response to a

determination that any of the responses from the untrusted mechanism is

an incorrect response, the untrusted mechanism to not be legitimate.

30.   (original) The computer readable medium of claim 29, wherein said sequence is

generated randomly.

31.   (original) The computer readable medium of claim 30, wherein said sequence is generated using a random number generator.

32.   (original) The computer readable medium of claim 29, wherein said sequence includes at least one submission of said first signature and at least one submission of said second signature.

33.   (original) The computer readable medium of claim 29, wherein the instructions for causing one or more processors to determine whether each response received from the untrusted mechanism is a correct response comprises:

instructions for causing one or more processors to determine, where the signature submitted to the untrusted mechanism was said first signature, whether the response from the untrusted mechanism is that said first signature is verified; and

instructions for causing one or more processors to determine, where the signature submitted to the untrusted mechanism was said second signature, whether the response from the untrusted mechanism is that said second signature is not verified.

34.   (new) A method for verifying the legitimacy of an untrusted mechanism, comprising:

submitting a sequence of submissions to an untrusted mechanism, wherein the sequence comprises at least two different submissions, wherein the

sequence is unpredictable to the untrusted mechanism, and wherein each

submission is submitted to the untrusted mechanism separately; and

for each separate submission in the sequence of submissions, performing steps

comprising:

receiving, from the untrusted mechanism, a response to the separate

submission;

determining whether the response is a correct response; and

in response to a determination that the response is an incorrect response,

determining the untrusted mechanism to not be legitimate.